Statement of Joseph S. Mahaley
Director, Office of Security
U.S. Department of Energy
before the
United States House of Representatives
Committee on the Budget
December 5, 2001

Mr. Chairman:

Thank you for the opportunity to appear before your committee today to speak with you about the Department of Energy and its response to the threat of terrorism since September 11th. I am Joseph Mahaley, Director of DOE's Office of Security. I report directly to the Office of the Secretary, and am responsible for the development of Department-wide policies governing the protection of national security assets under our charge. In addition to this policy development responsibility, my office is also charged with the conduct of security operations at DOE facilities in the Washington, D.C. metropolitan area.

The world as we know it changed on September 11th. After the attacks in New York and on the Pentagon, and with the threat of still a fourth plane headed east, DOE immediately went to Security Condition - 2 (SECON 2), our highest security level absent an imminent threat to a specified Departmental target. We shut down our shipments involving nuclear materials throughout the complex. General John McBroom is here today and is available to discuss the DOE response assets. While we have since stepped down from SECON 2, we remain on heightened security status, SECON 3, throughout the DOE complex. SECON 3 is our highest security level that can be maintained indefinitely. The DOE SECON system has served the Department well in that its purpose is to establish standardized protective measures for a wide range of threats, and to help disseminate appropriate, timely, and standardized information for the coordination and support of DOE crisis or contingency activities.

The highest level of protection in the DOE is associated with the protection of special nuclear material or SNM. The SNM in the Department ranges from complete nuclear weapons to the raw materials used to create the nuclear weapon. DOE refers to the protection program for this material as Nuclear Safeguards and Security. The DOE nuclear safeguards and security program is focused on the protection of the most critical nuclear assets and classified information, and is geared towards the prevention of the theft or unauthorized use of nuclear weapons and the prevention of acts of radiological sabotage. The worst case scenario that we protect against is an aggressive terrorist adversary. Our security forces are trained and performance tested against the terrorist scenario. Over 4,000 dedicated security personnel including approximately 3,500 armed officers are involved in our protection efforts. Additionally, more than 550 counterterrorism trained personnel at 11 separate locations are part of our Special Response Teams, our "SWAT" team equivalents. DOE also provides training and equipment to enable first responders to deal with a chemical or biological attack.

My office also manages a safeguards and security Technology Development effort. Its four key program elements include nuclear material control and accounting, physical security, information protection and counterterrorism. The Department is also fully involved and committed as a co-chair and funding provider to the Technical Support Working Group, the interagency counterterrorism research and development team, led by the State Department's Ambassador-at-Large for Counterterrorism. In addition to DOE's counterterrorism development projects, a key function of our Technology Development Program is providing a source of access and leveraging for the counterterrorism community to the resources of the DOE National Laboratories.

The events of September 11th dramatically changed our nation's threat environment, and as a result, has necessitated an examination of DOE's ability to respond to this new environment. To this end, we are working in conjunction with the Department of Defense to develop a combined Joint Threat Policy that will serve as the foundation of the protection strategy to be employed at all DOE and DOD nuclear facilities.

Prior to September 11th, the Department had just completed a review of security policies and procedures. Some very useful recommendations emerged from this

review that are currently being implemented. We will be looking more closely than ever at innovative approaches to our protection strategy. This will involve better use of technology, more and better training of our security employees, and more emphasis on security education and awareness among all employees.

In our continuing battle against the terrorist threat, we are working with Congress, the and other Federal agencies to include the FBI, DoD, Justice, and the NRC to enhance our security posture. We continue to work with other agencies as well. For example, we worked with the U.S. Postal Service and the Department of Health and Human Services to help them deal with the challenge of Anthrax-tainted mail. We are also supporting the newly established Office of Homeland Security in its critical role of coordinating the protection and emergency response assets across the Federal Government.

As the lead agency for coordinating Federal activities within the energy infrastructure, we are working closely with energy industry reps from oil, gas, and electric power industries to share information and help them assess their protection posture. We continue to work with state and local officials to address areas of concern that they might have and have provided technical expertise in the form of security assessments and recommendations to several states.

We have learned some valuable lessons since September 11th, particularly with respect to working in partnership with industry:

- First, cooperation and coordination with industry was excellent, primarily because of the crisis of the moment. However, we need more non-crisis dialogue. We also need clear and dedicated lines of communication. We have made substantial progress in this area in the past few months.
- Second, industry demonstrated willingness to share some information. They followed our lead in many respects and used our SECONs as a guide. In general, however, industry continues to express concern about sharing security-related information with the federal government for fear it might be made public through a Freedom of Information request. Third, the oil and gas industry recently established their Information Sharing and Analysis Center (ISAC). This needs to mature as quickly as possible to provide more

timely dissemination and analysis of information for this important energy industry segment.

- Fourth, we need to devise a workable way of sharing intelligence/threat data with industry. Addressing this issue is a DOE priority.
- Finally, we need standardized industry security levels and criteria so that when we go to a heightened security level, we will all know what that means. Industry has taken the initiative and is developing standardized security measures much along the lines of the DOE SECONs.

We have been busy, and will continue to be so for some time to come. We do not ever expect things to return to pre-September 11th "normal", because "normal" has now changed forever. Within DOE, there is a new paradigm, underscored most recently by Secretary Abraham when he told senior DOE leadership that he "...expects every manager to understand that they should instill a respect for and observe the highest standards of security."

We cannot control or alter the threats to the security interests entrusted to our care. What can be controlled, however, is our ability to plan and respond to threats, should they ever materialize. September 11th has fundamentally altered the Department's security perspective and posture. This is a significant challenge, but one that we are prepared to meet.